Liu, Vicky and Caelli, William and Smith, Jason and May, Lauren J. and Lee, Min Hui and Ng, Zi Hao and Foo, Jin Hong and Li, Weihao (2010) ***A secure architecture for Australia's index based e-health environment.*** In: Proceedings of The Australasian Workshop on Health Informatics and Knowledge Management (part of Australasian Computer Science Week ACSW 2010), 18-21 January 2010, Queensland University of Technology, Brisbane, Queensland.

A Secure Architecture for Australia's Index Based E-health Environment

Vicky Liu, William Caelli, Jason Smith, Lauren May,
Min Hui Lee, Zi Hao Ng, Jin Hong Foo and Weihao Li
Information Security Institute and Faculty of Science and Technology
Queensland University of Technology Australia
PO Box 2434 Brisbane, Queensland 4001, Australia

v.liu@qut.edu.au

Abstract

This paper proposes a security architecture for the basic cross indexing systems emerging as foundational structures in current health information systems. In these systems unique identifiers are issued to healthcare providers and consumers. In most cases, such numbering schemes are national in scope and must therefore necessarily be used via an indexing system to identify records contained in pre-existing local, regional or national health information systems. Most large scale electronic health record systems envisage that such correlation between national healthcare identifiers and pre-existing identifiers will be performed by some centrally administered cross referencing, or index system. This paper is concerned with the security architecture for such indexing servers and the manner in which they interface with pre-existing health systems (including both workstations and servers). The paper proposes two required structures to achieve the goal of a national scale, and secure exchange of electronic health information, including: (a) the employment of high trust computer systems to perform an indexing function, and (b) the development and deployment of an appropriate high trust interface module, a Healthcare Interface Processor (HIP), to be integrated into the connected workstations or servers of healthcare service providers. This proposed architecture is specifically oriented toward requirements identified in the Connectivity Architecture for Australia's e-health scheme as outlined by NEHTA and the national e-health strategy released by the Australian Health Ministers.

Keywords: architecture of health information systems, security for health information systems, health informatics, network security for health systems, trusted system, indexing based system for e-health regime, HL7.

1 Introduction

Undoubtedly, the adoption of e-health has much potential to improve healthcare delivery and performance (Goldschmidt 2005; AHM 2008). Anticipated improvements relate to better management and coordination of healthcare information and increased quality and safety of healthcare delivery. On the other hand, a security violation in healthcare records, such as an unauthorised disclosure or unauthorised alteration of individual health information, can significantly undermine both healthcare providers' and consumers' confidence and trust in the e-health system. A crisis in confidence in national e-health systems would seriously degrade the realisation of potential benefits.

Evidence from the NEHTA's Report on Feedback Individual Electronic Health Record (NEHTA 2008c) suggests that numerous healthcare consumers and providers embrace the adoption of national individual electronic health records because of the potential benefits. There are a number of consumers, however, who are reluctant to embrace e-health because of privacy concerns. Obviously, the security and privacy protection of information is critical to the successful implementation of any e-health initiative. NEHTA, therefore, rightly places security and privacy protection at the centre of its e-health approach.

In order to address the requirements for enabling a secure national e-health environment, we propose a security architecture based around the current strategic directions from the Australian Government's National E-Health Strategy (AHM 2008) and Connectivity Architecture (NEHTA 2008b) proposed by NEHTA, both recently released in December 2008.

This proposed architecture defines a model to support secure communications between healthcare providers and the Index System in the national e-health environment, which some other approaches fail to address. We draw on important lessons from the Internet's Domain Name System (DNS) for the development and deployment of the national healthcare Index System. Our approach embraces the hierarchical and distributed nature of DNS and defines the required components for a secure architecture for Australia's national e-health scheme. This proposed architecture employs a high trust computer platform to perform indexing functions and a high trust interface module as the application proxy to connect to the healthcare Index System and other healthcare service providers.

2 Paper Structure

This paper begins with a summary of the benefits associated with increased adoption of e-health; however, risks to privacy in such e-health systems must be addressed. Addressing the security appropriately is considered as key to success of the e-health implementation. Section 3 defines the paper's scope and

details our assumptions in the context of the Australian national e-health environment. Section 4 investigates three representative e-health initiatives resembling the approach being adopted in Australia. Section 5 reasons the lesson we can learn from Internet's DNS to design the national e-health Index System. The authors' proposal for a secure connectivity architecture with the required structures is described in Section 6. Section 7 illustrates a request for a specific patient's health records via the Index System with a set of information flows. The analysis of this work is incorporated in Section 8. Finally, the conclusion is drawn and future direction for work is outlined in Section 9.

3 Scope and Assumptions

The Australian National E-heath Strategy (AHM 2008) defines the basic building blocks for a national e-health system including: (1) the implementation of the healthcare identifier (HI) scheme for healthcare consumers and providers, (2) the establishment of standards for the consistent collection and exchange of health information, (3) the establishment of rules and protocols for secure healthcare information exchange, and (4) the implementation of underlying physical computing and network infrastructure. We propose a secure architecture to address the protection of clinical information exchange in a reliable and secure manner. This proposed architecture is specifically concerned with the secure architecture design and development to facilitate interactions between healthcare providers, healthcare organisations and the national Index System rather than focusing on healthcare consumers accessing healthcare information.

It is anticipated that the national HI scheme will be established by mid 2010 (AHM 2009). This paper assumes that an adequate national legislative framework will be established to support the management and operation of the healthcare identifier scheme (NHHRC 2009) to enable a national e-health implementation by July 2010. Presumably, the National Authentication Service for Health (NASH) becomes available for Public Key Infrastructure (PKI) services to support digital signing and data encryption in the national e-health environment. It is also assumed that the National Broadband Network (NBN) infrastructure will be constructed for electronically enabling access and transfer of health information nationally.

In the context of this paper, a service requester refers to the entity that uses a service provided by another entity. A service provider is an entity that offers a service used by another entity. A service provider can be a healthcare provider, healthcare organisation or organisation commissioned to provide services for healthcare providers or healthcare organisations.

4 Related Work

While most nations would appear to have some e-health initiatives at some stage of investigation or implementation, this section focuses on three national e-health architectures resembling the approach being adopted in Australia.

4.1 Dutch National E-health Strategy

The Dutch e-health infrastructure is constructed by the National IT Institute for Healthcare in the Netherlands (NICTIZ)[1]. The Dutch national e-health approach uses the National Healthcare Information Hub, National Switch Point (Landelijk SchakelPunt or LSP) to enable the exchange of healthcare information. There is no clinical information stored at the LSP. The clinical data details reside at local health information systems. The Dutch national index system, LSP, includes services such as identification and authentication, authorisation, addressing, logging and standardization of messages services (The Dutch Ministry of Health 2007)

The LSP links healthcare providers' information systems together to enable the electronic exchange of health information nationally. The Dutch national e-health network connectivity architecture requires the healthcare partitioners' health information system to comply with the security requirements for a "Qualified Health Information System to be allowed to connect to the LSP via a qualified commercial service provider. Such IT service providers are commissioned to provide secure communications between healthcare information systems and the LSP" (Spronk 2008) .

While the healthcare provider requests specific patient information which is located in other healthcare information systems, all queries are relayed via the LSP. The healthcare service provider responds to the LSP. Namely, the LSP aggregates the requested health data from the health service providers and then routes the health data to the requester. There is no direct communication between the healthcare service providing system and requesting system. The LSP also logs which healthcare practitioners have accessed patient data for accountability (The Dutch Ministry of Health 2007).

The Dutch national index system, LSP, is the central coordination point for exchange health information, including authentication, authorisation, routing and logging. Such an implementation model may appear suitable for a small scale of national e-health structure. Implementation of this model in a geographically large country will produce more network traffic, possibly creating performance bottlenecks; it is particularly prone to a single point of failure weakness.

4.2 National Health Service (NHS) in England

The National Health Service (NHS) in England implements the National Programme for IT (NPfIT) to deliver the central electronic healthcare record system. This central system is known as Spine. Spine provides national e-health services in England including:

- The Personal Demographics Service (PDS), which stores patients' demographic information including unique patient identifiers - NHS Numbers;
- Spine Directory Services (SDS), which provides directory services for registered healthcare providers and organisations;

[1] NICTIZ is Dutch national e-health coordination point and knowledge centre. The related information is available at http://www.nictiz.nl/, accessed 28/08/2009.

- National Care Record (NCR), which contains clinical information summaries as well as the location of the detailed healthcare information;
- Legitimate Relationship Service (LRS), which is an authorisation logic containing details of relationships between healthcare professionals and patients and patient preferences on information accessing; and
- Transaction and Messaging Spine (TMS), which provides routing for querying and responding to clinical messages via the NCR (Spronk 2007).

The English national e-health services include identification and authentication, authorisation logic, clinical summary information, directory services and routing. This programme is implemented in England, while Wales is running another national programme. The separate provisions of national e-health systems need to be made interoperable for information traversing across national borders.

4.3 USA Health Information Exchange (HIE)

USA National Institute for Standards and Technology (NIST) recently released a document entitled Draft Security Architecture Design Process for Health Information Exchanges (HIEs) (Scholl et al. 2009) to provide guidance for the development of a security architecture particularly for the exchange of healthcare information. The HIE security architecture design process includes five layers to construct a security architecture for healthcare information exchange. The five layers include: (a) policies for overall legal requirements to protect healthcare information access, (b) services and mechanisms to meet policy requirements, (c) operational specifications for the business processes, (d) definitions of technical constructs and relationships to implement enabling processes, and (e) provisions for technical solutions and data standards for implementing the architecture.

USA health information exchange architecture is based upon a hierarchical structure. Namely, it consists of a National Federation Health Information Exchange (HIE), Multi-Regional Federation HIEs, and Regional HIEs. The National Federation HIE, national federated technical architecture, connects a number of Multi-Regional Federation HIEs, involving multiple states jurisdictions. Multi-Regional Federation HIEs connect multiple regional HIEs. Regional HIEs can consist of two or more independent healthcare providers to share healthcare information. The participating healthcare providers set up their own trust agreement to define security and privacy requirements for the exchange of healthcare information (Scholl, Stine, Lin and Steinberg 2009) .

The Identity Federation Service provides identification and authentication services. The entity can be authenticated via the Identity Federation Service or its home organisation's authentication service to support single sign on for accessing the HIE services. The privilege management is performed by service providers locally (Scholl, Stine, Lin and Steinberg 2009).

The USA approach is different from the Dutch and English national e-health architectures. In a large nation like the USA, the distributed national e-health scheme seems suitable for scalability. USA e-health architecture is similar to the context of the DNS hierarchical model. This type of approach can mitigate the network traffic and performance bottleneck on the centralised e-health system.

5 Lesson Learnt from the Internet's Domain Name System (DNS)

The Internet's *"Domain Name System (DNS)"* has become a critical part of the Internet and of the *"World Wide Web (WWW)"* in particular. Without its services many current information systems and services provided over the Internet would not function. Indeed, as Web-based applications rapidly become the "norm", particularly in the public sector but also in the private sector, the resilience and high speed performance of the DNS have become mandatory requirements. The use of Web-based structures has been nominated as the basic functional structure of the Australia Federal e-health, NEHTA scheme. The DNS structure, determined some 25 years ago, is based around a globally distributed, hierarchical database architecture that relies upon replication for resilience and caching for performance. However, it has been realised that the basic DNS scheme is insecure, in the sense that both confidentiality and integrity, including authenticity and authorisation, were not part of the overall design during the original design and development time of the early to mid 1980s.

"Robustness and adequate performance are achieved through replication and caching" (Liu and Albitz 2006). Essentially, the client-server model chosen, via use of client "resolvers" and then "name-servers", has been proven over time and is the model suggested in this architecture. The hierarchical nature of the DNS structure again appears suitable given that the Australian system must cater for a federated national structure with roles for the various State level participants. The *"ccTLD"* or *"country top level domain"* coupled with a "2nd level" structure appears to offer suitable benefits in organisation and management as well as the necessary backup resilience that is required in the overall scheme.

The appropriate security arrangements, the *"Transaction Signatures (TSIG)"* structure based on a single-key cryptographic system again helps in this regard in relation to the secure synchronisation of actual DNS nameserver systems themselves. As Liu and Albitz (2006) state, *"TSIG uses shared secrets and a one-way hash function to authenticate DNS messages, particularly responses and updates."* Similar schemes exist for confidentiality, integrity and authenticity services in data networks in the banking and finance sector.

As mentioned above, the original DNS structure did not consider matters of confidentiality and integrity. At the same time, the TSIG scheme is not scalable to any real dimension as nameservers correspond with an arbitrary set of other nameservers. The *"DNS Security Extensions (DNSSEC)* (Arends et al. 2005a; Arends et al. 2005b; Arends et al. 2005c)*"*, through use of "Public Key Cryptography", enable DNS "zones" to "digitally sign" the necessary nameserver tables so that, on distribution, such tables can be checked for authenticity and integrity by the receiver. The addition of appropriate DNSSEC records to the overall database structure provides a useful

model that may be incorporated into the proposed architecture that is the subject of this paper.

In summary, the overall DNS experience, and the structure of the DNSSEC security extensions provide a most suitable model for incorporation, in modified form, into the healthcare index architecture proposed. The DNSSEC structure assists in combating known attacks on the Internet system through such techniques as "cache poisoning", "traffic diversion", "man-in-the-middle attacks" and so on. At the same time, however, the basic index systems, like the Internet's DNS nameserver systems, must be installed and managed on basic computer systems, including the necessary operating systems (OS) that are sufficiently secure for the purpose. The immediate use of DNSSEC style structures is seen as essential given that many aspects of the proposed e-health record infrastructure will reside on the general purpose Internet.

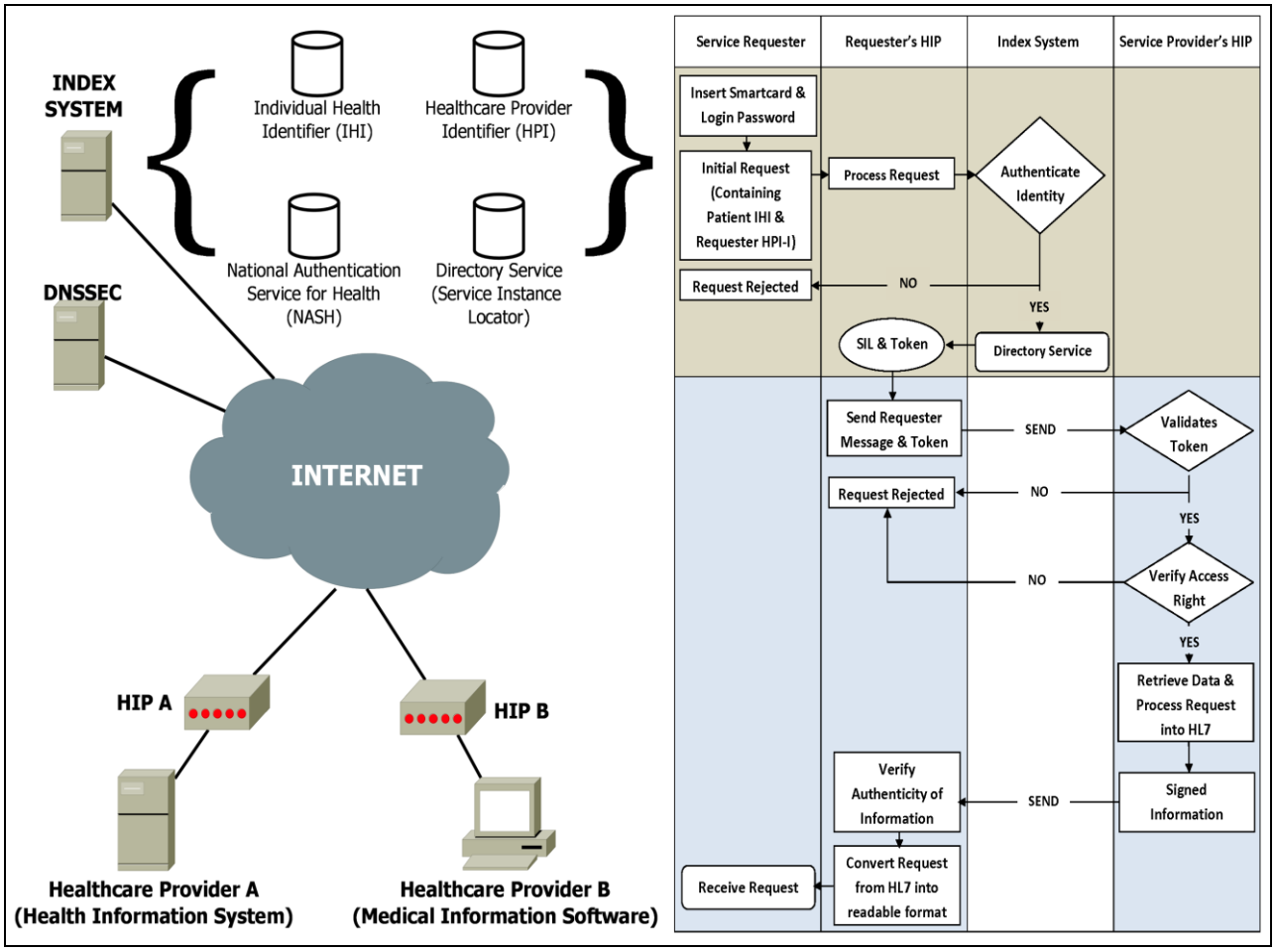

Figure 1 Proposed Architecture Overview and Key Information Flows

6 Our Approach

Generally, health information is stored over a number of different health information systems. A national index system must be available for the provision of directory services to determine the distributed locations of the source systems holding the related health records. Our proposal addresses this need by defining a model to support secure communications between healthcare providers and the Index System in the national e-health environment as shown in Figure 1. This proposed architecture is based on the broad architecture of the Australian Government's National E-health Strategy (AHM 2008) and NEHTA's Connectivity Architecture (NEHTA 2008b), both released in December 2008.

Our proposed architecture defines the required constructs to share and transfer healthcare information securely between healthcare providers and the authorised national Index System. This architecture proposes that the Index System should be built on a high trust computer platform as well as mandating that the participating healthcare provider's need to adopt a high trust interface module - HIP as the application proxy to link to the Index System and other health information systems. Additionally, the authors argue that a fundamental security issue, that of name resolution, must be addressed prior to the interactions between the healthcare providers and national Index System. This paper, therefore, proposes a trusted architecture not only providing the indexing service but also incorporating a trusted name resolution scheme for the enforcement of communicating to the authorised Index System.

Since the Index System is itself a critical application under any operating system, that Index System must be protected from even internal threats through the use of modern "flexible mandatory access control (FMAC)" structures. Under such an operating system, and as distinct from the less secure "discretionary access control (DAC)"

systems, even a systems manager may not have permission to access the health record data. In simple terms, in these systems there is no "super-user" capable of obtaining access to all system resources at any time. If an individual nameserver system is "captured", propagation of exposure will not extend beyond the compromised application itself, a vital concern in any e-health record indexing structure. Such systems exist and are commercially available, e.g. the "Secure LINUX (SELinux)" systems, "Solaris/SE" system, etc. The proposed "HIP" structure would make use of such security enforcement to provide the necessary protection levels.

6.1 Index System (IS)

The authors argue that the load of the national Index System should be relatively lightweight to perform e-health indexing services efficiently. This can mitigate the Index System explosion and traffic bottleneck risks. Such an approach is favourable in a geographically large country such as Australia. To maximise the efficiency of the indexing services, the proposed Index System does not provide network connectivity services, messaging translation, addressing and routing functions and extensive logging of all message access. These services can be performed at the level of the local health information systems via the HIP, which is detailed in Section 7.2. The access control and authorisation process is best performed close to where the source system is, as each healthcare service provider might implement the service differently based on its own health information system access requirements. NEHTA (NEHTA 2008b) also states that there are no centralized network provisions to handle peer-to-peer communications; each service must manage its own interface to the network.

The Index System will be a centralised facility run at a national level. It is envisioned that the directory service is devised in the context of a DNS, which uses hierarchical distributed database architecture.

Our proposed national Index System performs common and fundamental functionalities including:

- Identification and authentication, and
- Directory services.

6.1.1 Identification and Authentication Services

The national Healthcare Identifiers Service (HI Service) is indeed one of the building blocks for the national e-health infrastructure. The national HI scheme for identification services must be deployed prior to the implementation of the national e-health system. The HI Service will provide accurate identification of individuals and healthcare providers in the national e-health environment.

Individuals receiving healthcare services will be assigned an Individual Healthcare Identifier (IHI). All authorised Healthcare providers will receive a Healthcare Provider Identifier – Individual (HPI-I). Healthcare centres and organisations in Australia will be provided with a Healthcare Provider Identifier – Organisation (HPI-O). To be eligible to query the HI Service, a requesting entity must be nominated by a healthcare organisation and have an HPI-I associated with an HPI-O. The IHI Service will allow authenticated healthcare providers to lookup a specific IHI. The HPI Service of the Index System will provide lookup services to navigate the locations of healthcare providers to facilitate communication and the exchange of healthcare information (AHM 2009).

National Authentication Service for Health (NASH) is designed by NEHTA to provide PKI authentication services. NASH will issue digital certificates and tokens for registered and certified healthcare providers and organisations (AHM 2009).

6.1.2 Directory Services

The Directory Service is one of the fundamental services in national e-health infrastructure. Since healthcare data are located at various places, directory services are used to identify and locate the available information. The Directory Service in the Index System provides a mechanism for obtaining the necessary information for invoking a service. This information contains the network location of the service, the digital certificate required to use it and other information required to invoke the service. It is envisaged this will be specified in Web Services Description Language[2] (WSDL) format, which equates to Service Instance Locator (SIL) (NEHTA 2008d) functionalities outlined by NETHA.

6.1.3 Operation of the Directory Services

Based upon NEHTA's definitions (NEHTA 2008a) on concepts and patterns for implementing services, the service patterns can be divided into two broad categories: synchronous and asynchronous services. A synchronous service occurs in direct response to a request. An asynchronous service has no relationship between the events. For example, to request a specific individual's health records is a synchronous service. To send out a discharge summary report to a healthcare provider is an asynchronous service.

With a synchronous service, when interacting with the directory service the requesting entity will provide proof of their identity (HPI-O) and the IHI associated with the records they are requesting. Once the requester has been authenticated by the Index Server, it will respond with the following: (a) a signed token attesting to the identity of the requester ($\{token\}Sign_{IS\_PrivKey}$) and (b) a list of service instances containing health records for the person identified by the IHI (Service_Instance_1,...,Service_Instance_N).

The entire response is signed so that the requester can be assured that it is a legitimate response from an authorised Index System and that any alterations to the response will be detectable. The response is also encrypted under a key known by the requester ($\{...\}Encrypt_{HPI\text{-}O\_PubKey}$), in order that the confidentiality of both the requester and the individual identified by the IHI is maintained.

[2] WDSL is used for describing how to access the network services in XML format. More detail is available at http://www.w3.org/TR/wsdl#_introduction accessed 30/08/2009.

The token is signed independently of the entire response in order that it can be reused with requests to each service instance. The full response is depicted in Figure 2.

$$\{\{token\}Sign_{IS\_PrivKey}, Service\_Instance\_1, ..., Service\_Instance\_N\}Encrypt_{HPI\text{-}O\_PubKey}$$

Figure 2: Service Instance Response Message Format

The service instance information contained in the response identifies the target system location and information necessary for securely invoking that service. This may include, but will not be limited to the credentials / certificates required to access the service. The signed token provided in the Index System response may be the only credential required, in which case the effort expended by the Index System in authenticating the requester is reused. It is, however, conceivable that additional authentication may be required by a given service instance. For example, the requester may need to prove that they are a member of a given practice or college of medical practitioners.

With an asynchronous service, such as when a discharge summary message needs to be sent to the patient's primary healthcare provider, the healthcare provider issuing the summary queries the Index System for the primary healthcare provider's HPI, location and the digital certificate and then signs and encrypts the discharge message prior to transmission.

6.2 Healthcare Interface Processor (HIP) – Proxy Service

Our design philosophy of HIP draws on principles used in the Interface Message Processor (IMP) of the Advanced Research Projects Agency Network (ARPANET). Each site uses an IMP to connect to the ARPANET network in order to isolate the potential hostile system connecting the ARPANET network. Our design rationale underlying HIP is to provide a secured communication channel for an untrusted health information system connected to the Index System as well as for health information exchange between healthcare providers. Wherever a connection to the national indexing system is required, a HIP facility has to exist. The design goal for HIP is to make it as a "plug and operate" facility, which is easy and simple to use for healthcare providers as well as with characteristics of high security, reliability, efficiency and resilience. Such a design would be very beneficial and useful particularly for healthcare providers.

HIP contains its own on-board crypto-processor based on a trusted computing based module to store cryptographic keys. Any information system depends, therefore, upon a trusted base for safe and reliable operation, commonly referred to as a "trusted computing-base". Without a trusted computing base any system is subject to compromise. For this reason HIP aims to run on top of trusted hardware, firmware and operating system. HIP, a self-contained unit configured with an IP address, is capable of running Web services. HIP carries out its works from layer 1 to 7 of the seven-layer OSI model.

It is envisaged that HIP achieves provisions of security services and mechanisms based upon the security and management concepts of the OSI IS7498-2, including:

- To establish a **trusted path** to connect to the authorised Index System,
- To provide **peer-entity authentication** between healthcare providers and national Index System,
- To facilitate **secure healthcare information exchange** in transit,
- To provide **data protection** with appropriate **access control** mechanisms,
- To provide **interoperability** to enable healthcare information exchange between disparate healthcare systems with varying security mechanisms,
- To support **accountability** when healthcare information has been accessed, and
- To provide **operation flexibility** with "emergency override" and **capacity flexibility** for various scales of healthcare organizations.

6.2.1 Trusted Path Establishment

In response to the recent increase in DNS cache poisoning and traffic diversion attacks, we propose that the first step is to perform the enforcement of communicating to the authorised Index System prior to the interactions between the service requesting entity and the Index System. To achieve this, from a technical underlying process, HIP should be pre-configured to contact a DNSSEC capable server to perform a trusted name resolution in order to defend against false DNS data and assure that connections are only established with the legitimate Index System.

6.2.2 Peer-Entity Authentication

Many proposals are only concerned with the authenticity of the requesting entity (i.e. one-way authentication) but fail to address the importance of two-way authentication. Our proposed architecture provides a mutual peer-entity authentication service complying with the ISO 7489-2. To authenticate the authenticity of the Index System, the service requesting entity must validate the certificate of the Index System. Once the authenticity of the national Index System is assured, the Index System authenticates the identity of the healthcare service requesting entity. In this sense, the authentication service of the Index System acts as a notarization mechanism in line with the philosophy of peer-entity authentication stated in ISO IS7498-2.

6.2.3 Secured Communication Channel for Health Information Exchange

The healthcare provider's computer may have its security compromised. HIP, a hardened and qualified facility, acts as a proxy server establishing a secured communication channel connecting to the Index System and bringing isolation from the untrusted computer.

HIP will be assigned a standard unique identifier (i.e. HPI-O) and be issued an asymmetric key pair for digitally signing and encrypting to achieve integrity and confidentiality goals. HIP contains its own on-board crypto-processor, thus it can facilitate the secure exchange of health information. In addition, HIP is built on the

Trusted Platform Module (TPM) that is used to store cryptographic keys.

6.2.4 Provision of Data Protection

As various healthcare organisations may have their own specific access authorisation requirements and processes, access authorisation is best performed where the resource system is located. Once the requesting entity's identity is authenticated, the request of particular healthcare information is presented to the target service provider. The HIP of the target service provider will provide the verified identity and the profile of the requester to the authorisation logic unit to perform access decision making. The authorisation decision depends upon the requesting entity's profile and defined privilege management policy. The implementation of the authorisation logic unit is based on the "Sensitivity Label" function outlined by NEHTA (NEHTA 2008c).

6.2.5 Interoperability Platform

NEHTA[3] is responsible for selecting electronic messaging standards in Australia's health sector. It has endorsed Health Level 7 (HL7) [4] as the national standard for the electronic exchange of health information. HIP provides an interoperability platform by incorporating an HL7 Interface Engine and Message Mapping Sets conforming to the HL7 v3 Message Standards for healthcare information exchange. HIP also incorporates an HL7 Interface Engine and Message Mapping Sets for messaging Interoperability.

HL7 Interface Engine

Any non-HL7-compliant data contents are translated into the HL7 standard format (XML-based data structure) by the HL7 Interface Engine prior to information transmission. The HL7 Interface Engine contains a set of mapping algorithms to map data contents with an appropriate HL7 Message Template to generate an HL7 message.

Message Mapping Sets

The Message Mapping Sets contain a repository of HL7 Message Templates for various clinical and administrative messages. Each set provides one HL7 Message Template to serve for one clinical or administrative message. Message Mapping Sets will be designed and developed to meet the current healthcare service needs and will be imported into HIP. The HL7 Message Template guides and directs data contents to form an HL7 message.

HL7 Clinical Document Architecture (CDA)

HL7 Clinical Document Architecture (CDA) provides a framework for clinical document exchange. HIP imports the HL7 message into a CDA document. This CDA document is also associated with an appropriate stylesheet. The CDA document and the stylesheet will be sent to the requesting entity through Web services. The requesting entity renders the received document with the stylesheet in a human-readable form with a Web browser.

6.2.6 Privacy Accountability

Audit trail mechanisms can be used to deter unauthorised access to data to improve privacy accountability. To enforce privacy accountability, HIP could be configured to automatically trigger an audit trail event particularly when data is being accessed.

6.2.7 Operation and Capacity Flexibility

HIP aims to accommodate emergency override whereby any delays that may potentially occur through authentication and authorisation may be overridden. This is particularly relevant in the case of defined emergency including pandemic circumstances. HIP is designed to provide an emergency override provision called "Hit-the-HIP" for ease of operation.

The HIP architecture is flexible enough to cater for interfacing at various levels. Examples of healthcare organisational structures include a one-person general practice clinic, and small or medium clinics to large hospitals. It is proposed that a number of design variations for the HIP facilities, depending on the healthcare structure, may include:

- One-person healthcare practitioner,
- Smaller healthcare practitioners,
- Hospital administration, and
- Regional hospital administration

7 Envisioned Key Information Flows

This section uses a scenario to illustrate the key information flows (see Figure 1) based on the proposed architecture described in Section 6. While a requester needs to inquire about a specific patient's health information, the key information flows of the interactions between the requester, Index System and service provider are illustrated in the following steps. Note that all request and response messages prior to transmission are signed and encrypted for confidentiality, authentication and message integrity reasons.

1. **Peer-Entity Authentication Process**
   - 1.1. Prior to peer-entity authentication, to ensure the secure resolution, the service requester's HIP obtains the address of the Index System from the DNSSEC system which is pre-configured in the HIP.
   - 1.2. The service requester initiates a connection with the Index System via the service requester's HIP. To ensure the authenticity of the Index System, the service requester's HIP validates the certificate of the Index System.
   - 1.3. To ensure the identity of the service requester, the service requester logs into the Index System with his/her smart card containing their credentials.
2. **Health Record Enquiry Process**

[3] NEHTA Sets Direction for Electronic Messaging in Health is available at http://www.nehta.gov.au/nehta-news/423-nehta-sets-direction-for-electronic-messaging-in-health, accessed 19/08/2009

[4] Health Level 7, an American National Standards Institute accredited standard, has been developed to enable disparate healthcare applications to exchange key sets of clinical and administrative data.

2.1. The service request, containing the patient's IHI and requester's HPI-I, is sent to the Directory Services of the Index System to inquire which health providers hold the health records of the specific patient.

2.2. The Directory Services of the Index System responds with a token and a list of the service instance information for service invocation to the requesting entity. This token indicates the requester identity assertion to enable single sign on for service invocation.

2.3. The requester verifies the received information and then contacts each target service provider for service invocation. The requester sends the request including the token with other necessary information to invoke the service.

3. Verification and Authorization Evaluation Process

3.1. Each target service provider validates the request message containing the token and other necessary information for service invocation.

3.2. In turn, the request is passed to the authorization logic to make an access authorisation decision based on the service requester's profile indicated in the ticket and any additional authorisation attributes which are mutually agreed by the policy.

4. Provision of Requested Health Record Process

4.1. If the access is granted, the service provider extracts the health record from the data source.

4.2. The service provider processes the requested health record into the HL7 message format.

4.3. The target service provider sends the signed and encrypted information to the requester.

4.4. The service provider records the information access for auditing purposes.

5. Reception of Requested Health Record Process

5.1. The requested information arrives at the service requester's HIP.

5.2. The service requester's HIP verifies the information arrived and then extracts the requested information which is in HL7 message format.

5.3. The message must be presented in a human readable format. The representation of HL7 message is rendered and displayed to the requester.

8 Analysis

A first point of contact in any Index System must be itself verified for authenticity and integrity. In Internet terms the client system must be sure that it is connected to the correct Index System and not to some fraudulent system or via some intermediate node point capable of monitoring all traffic. The suggestion for use of a DNSSEC style structure in the overall architecture is seen as a minimum requirement for overall trust in the system.

In turn, this implies that all systems used in the creation and operation of a "centralised" Index System must be security verified in line with accepted international standards. The main such standard is the *"Common Criteria (CC)"* set, [5] under international standard IS-15408, accepted by many nations [6] as the base for evaluation of the security stance of any system. Isolation of critical security functions into verifiable hardware and software structures capable of CC *"protection profile"* definition is envisaged along with the acceptance of a requirement for an associated evaluation at a minimum of an evaluation level of "EAL5". This would apply to the HIP. It should also be a requirement that the USA's "FIPS 140-2", the Federal Information Processing Standard, be used for the security verification of cryptographic functions, in line with accepted industry practice.

Unlike previous structures, the HIP may operate at all seven layers of the OSI model and, indeed, be seen as a "proxy" for Internet interaction. For example, the functionalities of HIP include:

- Routing control functions operating at layer 3, the "network layer" of the OSI model;
- HL7 interpreter functions working at the "presentation layer", layer 6;
- Web service operations carried out at layer 7 of the OSI model, the "application layer"; and
- The encryption/decryption mechanisms at layers 2, 3 and 4 of the OSI model.

The proposed structure is cognisant of NEHTA's architectural designs for the overall national health record index scheme proposed for Australia. Moreover, the main aim of the HIP concept is to simplify overall security control and management of the e-health environment from the point of view of those health professionals and practitioners who will be using the system in the future. The whole HIP architecture is seen as being able to be explained and understood by health professionals and related people who are not ICT experts. Moreover, the HIP and its security should be transparent to them in normal operation. The goal of the proposed system is to make the HIP understandable and essentially transparent to users so that health practitioners can focus on their primary functions to deliver quality healthcare service. In this regard, control and management of the overall system is vested in appropriate information and network systems professionals, not the end users or health partitioners themselves.

9 Conclusion and Future Work

This paper proposes three distinct suggestions on the architecture set:

(1) Trusted domain name services are a critical element in the overall trusted architecture of any indexing based healthcare systems to combat name resolution cache poisoning and traffic diversion attacks;

---

[5] The Common Criteria Portal is available at – http://www.commoncriteriaportal.org, accessed 7/09/2009.

[6] More information about the Mutual Recognition and the Common Criteria Recognition Arrangement is available at http://www.dsd.gov.au/infosec/evaluation_services/aisep_pages/aisep_partners.html accessed 07/09/2009.

(2) A trusted architecture for the Index System which provides the critical solution to determine the locations of distributed health records. This Index System plays a vital role in the national e-health scheme for identification and authentication and directory services. The Index System, therefore, must be a high trust system running on a trusted platform; and

(3) HIP plays a vital role as a proxy server connecting to the national Index System as well as linking to untrusted health information systems. The proposed "HIP" structure will be built on top of a trusted platform. This makes use of available security enforcement to provide the necessary protection levels.

We envisage that the HIP would be subject to security functionalities and evaluation at the minimum requirements of EAL5 under the Common Criteria/ISO15408[7], in which Australia participates under the Common Criteria Recognition Agreement (CCRA)[8].

There are a number of proposals to maintain summarised healthcare records within the overall index system/switching system (Spronk 2007; Spronk 2008). A summary of healthcare records in Australia is called an Individual Electronic Health Record (IEHR) (AHM 2008). Our architecture can accommodate IEHR: for example an IEHR database added in Figure 1. This proposal needs to be further examined in light of prior experience in other sectors, such as banking and finance industries. While it would appear possible to maintain IEHRs within the national Index System, practicality may indicate that, in line with the DNS system discussed in this paper and in the banking sector, IEHRs may be best implemented at the point where such aggregation is most feasible. In Australia, this would indicate, in light with the DNS system, a second level Index System at the state level which would also contain IEHRs. Under investigation in the overall project is the feasibility of aggregating IEHRs on demand for the use of point access.

Point of Sale (EFTPOS) is a model that can be used to develop HIPs. Part of our future work is to design a prototype to demonstrate this. This paper forms a foundation for the creation of such a prototype/demonstrator high trusted Index System coupled with a prototype HIP. This will form a base of future requests for research funding. HIP will be developed as proof-of-concept which may be used when tendering for supply and installation. It is suggested that the government will issue the development and testing of HIP which involves the production of 5-6 laboratory prototypes and 50-100 production prototypes. Upon the successful bidder testing, this proposal suggests that the government would issue tenders for the production and installation of HIP. This is based upon the successful experience in the financial sector, in particular, the successful structure and deployment of Australian Electronic Funds Transfer at EFTPOS systems over the last 25 years.

Although this paper concentrates on the Australian national e-health environment from a security perspective, our conclusions could be equally applied to any distributed, indexed based healthcare information systems involving cross referencing of disparate health data collections or repositories.

[7] The international standard ISO15408 sets a strict guideline for evaluating security policy, program design documents, source code, manuals and other factors.

[8] The Common Criteria Recognition Agreement (CCRA) Web site is available at http://www.commoncriteriaportal.org/theccra.html, accessed 03/09/2009.

10 References

AHM (2008): National E-Health Strategy Summary. http://www.health.gov.au/internet/main/publishing.nsf/Content/604CF066BE48789DCA25751D000C15C7/$File/Summary%20of%20National%20E-Health%20Strategy-final051208.pdf. Accessed 21/08/2009.

AHM (2009): Healthcare Identifiers and Privacy: Discussion paper on Proposals for Legislative Support. www.health.gov.au/.../Typeset%20discussion%20paper%20-%20public%20release%20version%20070709.pdf Accessed 13/08/2009.

Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S. (2005a): RFC4033 DNS Security Introduction and Requirements. http://www.ietf.org/rfc/rfc4033.txt. Accessed 07/09/2009.

Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S. (2005b): RFC4034 Resource Records for the DNS Security Extensions. http://www.ietf.org/rfc/rfc4034.txt. Accessed 07/09/2009.

Arends, R., Austein, R., Larson, M., Massey, D. and Rose, S. (2005c): RFC4035 Protocol Modifications for the DNS Security Extensions. http://www.ietf.org/rfc/rfc4035.txt. Accessed 07/09/2009.

Goldschmidt, P. G. (2005): HIT and MIS: Implications of Health Information Technology and Medical Information Systems. http://delivery.acm.org/10.1145/1090000/1089141/p68-goldschmidt.pdf?key1=1089141&key2=5606972511&coll=portal&dl=ACM&CFID=15151515&CFTOKEN=6184618. Accessed

Liu, C. and Albitz, P. (2006). DNS and BIND, O'Reilly Media Inc.,.

NEHTA (2008a): Concepts and Patterns for Implementing Services Version 2.0 draft - 1 September 2008 Draft for Comment. http://www.nehta.gov.au/component/docman/doc_download/547-service-instance-locator-requirements-v10-draft-archived. Accessed 09/09/2009.

NEHTA (2008b): Connectivity Architecture Version 1.0 - 1 December 2008 Release. www.nehta.gov.au/component/.../624-connectivity-architecture-v10-. Accessed 18/08/2008.

NEHTA (2008c): Report on Feedback Individual Electronic Health Record, issued by the National Health and Hospitals Reform Commission

NEHTA (2008d): Service Instance Locator: Requirements. www.nehta.gov.au/.../606-service-instance-locator-requirements-v11 Accessed 01/09/2009.

NHHRC (2009): A Healthier Future for All Australians – Final Report

http://www.nhhrc.org.au/internet/nhhrc/publishing.nsf/Content/nhhrc-report. Accessed 13/08/2009.

Scholl, M., Stine, K., Lin, K. and Steinberg, D. (2009): Draft Security Architecture Design Process for Health Information Exchanges (HIEs). http://csrc.nist.gov/publications/drafts/nistir-7497/Draft-NISTIR-7497.pdf. Accessed 5/09/2009.

Spronk, R. (2007): The Spine, an English National Programme. http://www.ringholm.de/docs/00970_en.htm. Accessed 30/08/2009.

Spronk, R. (2008): AORTA, the Dutch National Infrastructure. http://www.ringholm.de/docs/00980_en.htm. Accessed 30/08/2009.

The Dutch Ministry of Health (2007): Overview of the Architecture on Dutch National E-health. http://www.uziregister.nl/Images/emd_wdh_uk_tcm38-17362.wmv. Accessed 25/08/2009.